

secret information derived from secret information provided to a key recovery agent. . . . It is further contemplated that Law Enforcement, with a valid court order or warrant, can obtain the necessary key-encrypting keys from the key recovery agents, thereby allowing them to decrypt the encrypted data keys that are appended to the encrypted messages and in turn to decrypt the encrypted communications or mail."

Jakobsson, as cited by the Office Action, teaches techniques for redistributing mail messages to secondary recipients when a primary recipient is not available by transforming a message encrypted for a first recipient to messages that are encrypted for the respective secondary recipients.

Both Gennaro and Jakobsson teach techniques for encrypting and decrypting a document so that the document may be transmitted securely. However, both Gennaro and Jakobsson are silent regarding how to securely view the document once the document is received.

By contrast, embodiments according to the subject matter of the pending claims prevent a decrypted copy of the transferred document from being available for electronic copying by an intruder, or the intended recipient. This is accomplished by decrypting the document within the viewing, or rendering application. The proxy key transformation and the session key decryption is performed within the viewing application only and at no time is any decrypted portion of the document stored in a manner that would allow unauthorized copying.

For example, independent claim 1 recites a method for using a partially encrypted document that includes among other features, issuing a document usage request for using the partially encrypted document in a session; rendering a non-encrypted portion of the partially encrypted document; performing a proxy transformation on the partially rendered, partially encrypted document using the proxy key; and decrypting the proxy transformed, partially rendered, partially encrypted document using the session key, wherein the proxy key and the

session key may be used to decrypt the partially encrypted document as part of the session rendering process only, thereby assuring that only rendered images of the decrypted document are available to an end user.

During the June 8 interview, Applicants representative asserted, and the Examiners agreed, as reflected in the Interview Summary prepared by the Examiners, that neither Gennaro nor Jakobsson teach such a feature.

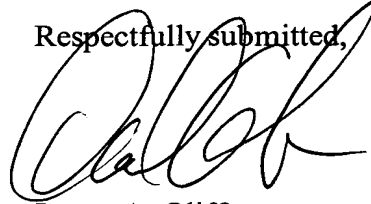
For at least these reasons, it is respectfully submitted that independent claim 1 is patentably distinguishable over the applied art. Independent claims 6 and 13 include features similar to those addressed above with respect to claim 1 and, therefore, are patentably distinguishable over the applied art for at least the reasons addressed above with respect to claim 1. Claim 2-5 and 7-12 depend from claims 1 and 6, and are, therefore, patentably distinguishable over the applied art for at least the reasons discussed above with respect to claims 1 and 6, as well as for additional features they recite.

Accordingly, reconsideration and withdrawal of the rejection of claims 1-13 are respectfully requested.

In view of the foregoing, it is respectfully submitted that this application is in condition for allowance. Favorable reconsideration and prompt allowance of claims 1-13 are earnestly solicited.

Should the Examiner believe that anything further would be desirable in order to place this application in even better condition for allowance, the Examiner is invited to contact the undersigned at the telephone number set forth below.

Respectfully submitted,



James A. Oliff  
Registration No. 27,075

Daniel A. Tanner, III  
Registration No. 54,734

JAO:JMH/jam

Date: July 5, 2006

**OLIFF & BERRIDGE, PLC**  
**P.O. Box 19928**  
**Alexandria, Virginia 22320**  
**Telephone: (703) 836-6400**

<p>DEPOSIT ACCOUNT USE AUTHORIZATION Please grant any extension necessary for entry; Charge any fee due to our Deposit Account No. 24-0037</p>
--